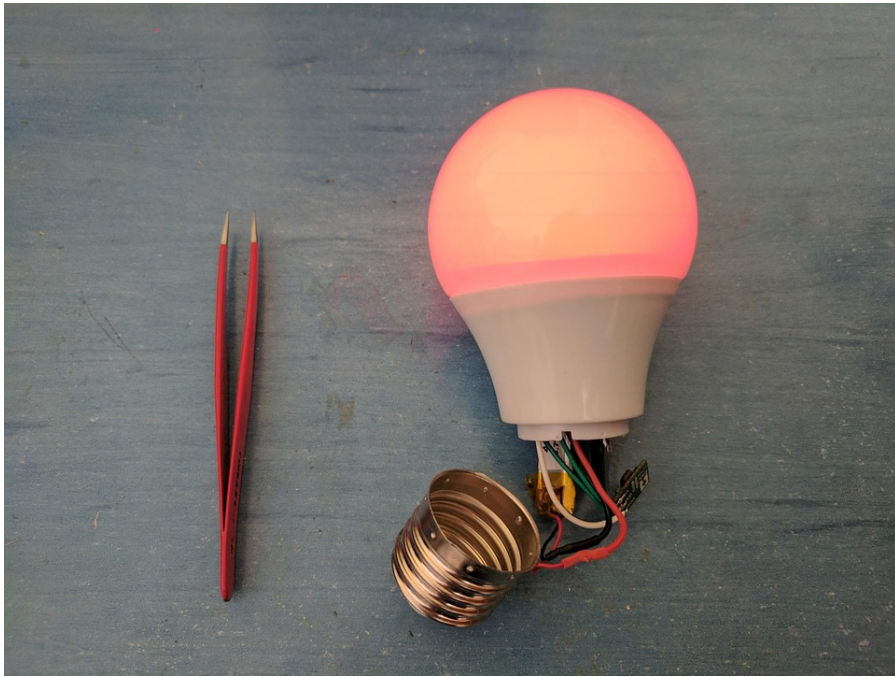


La problématique des objets connectés trop indiscrets



La
problématique
des objets
connectés
trop
indiscrets

Brancher le baby phone, activer le thermostat, prendre sa tension ou sa température... Gestes loin d'être anodins dans l'internet des objets.

On a récemment évoqué dans les médias le danger potentiel d'un aspirateur automatique baptisé Roomba. Ses algorithmes et capteurs détectent les objets et obstacles, de manière à établir une cartographie des pièces où il est utilisé. Chez le fabricant, on précise que ces données servent à améliorer le matériel. Les détracteurs prétendent que les données récupérées sont vendues. Peu importe, la prudence s'impose avec les objets du quotidien connectés sur Internet.

Pas de budget pour la sécurité

Frigos, pacemakers, smartwatches, babyphones et téléviseurs derniers cris peuvent désormais présenter un danger. Samsung conseille ainsi de désactiver la reconnaissance vocale sur ces Smart TV afin d'empêcher que vos conversations privées puissent être interceptées! Ces TV intelligentes disposent de deux microphones; un à l'intérieur du téléviseur, l'autre à l'intérieur de la télécommande afin d'interagir avec votre Smart TV à la voix. Un fournisseur de services tiers convertit vos commandes vocales interactives en texte et dans la mesure nécessaire pour vous fournir les fonctionnalités de reconnaissance vocale. Le fabricant insiste sur le fait qu'il utilise le cryptage standard de l'industrie pour sécuriser les données.

Multinationales ou start-up mettent aujourd'hui sur le marché des produits connectés où la sécurité pour protéger les données est reléguée au second plan pour des raisons de budget. Ces appareils disposent de petits processeurs capables de traiter un nombre d'instructions limité. Au point qu'aujourd'hui l'industrie récompense les personnes aidant à remonter des bugs de sécurité (sites, applications etc.) via les bug bounty qui mettent en contact ceux qui cherchent et trouvent les failles avec les développeurs de produits. Une stratégie préventive de sécurité qui en appelle d'autres...[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

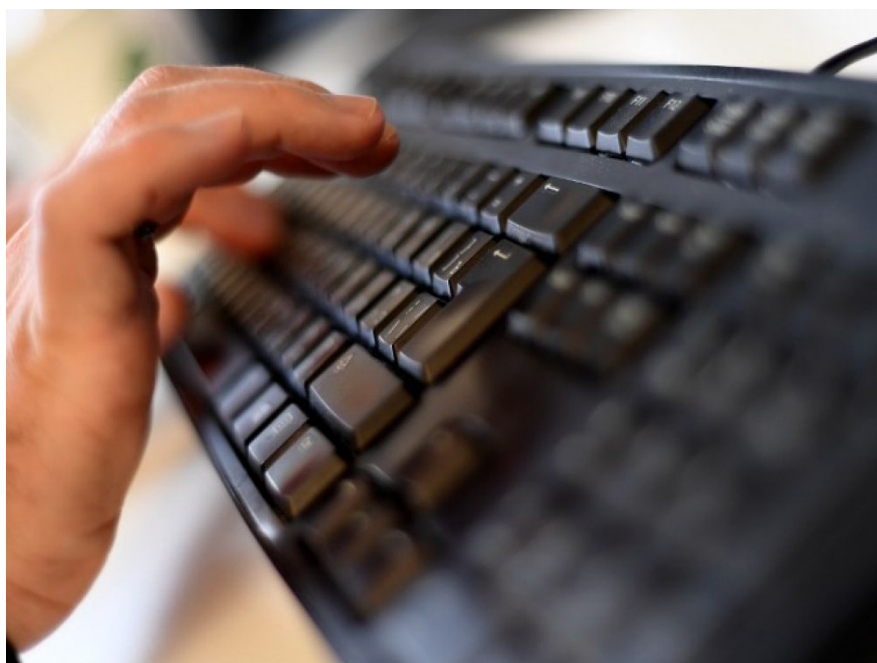


[Contactez-nous](#)

Réagissez à cet article

Source : *La problématique des objets connectés trop indiscrets*
– *Toute l'actu 24h/24 sur Lavenir.net*

Cyberattaques : pourquoi s'assurer n'est pas la meilleure solution



Cyberattaques :
pourquoi
s'assurer
n'est pas la
meilleure
solution

Les risques de cybercriminalité sont l'une des bêtes noires des entreprises. Les cyberattaques deviennent de plus en plus nombreuses et coûteuses. Face à cette situation, s'assurer n'est pas forcément la meilleure solution.

Les cyberattaques seront de plus en plus coûteuses et de plus en plus nombreuses à l'avenir. Au cours des dernières années, les offres d'assurances anti-cyberattaques, les cyberassurances, ont fleuri dans le monde. Le problème, c'est que les risques de cyberattaques sont pour la plupart difficilement chiffrables car ils peuvent avoir un impact sur de nombreux aspects de la vie d'une entreprise, comme sa réputation ou son image. Dès lors, la problématique assurantielle devient un véritable casse-tête. Car plus le risque est important et plus la police d'assurance sera chère. Va-t-on se diriger vers des assurances qui ne couvriraient que la moitié du risque ? Les risques devenant plus coûteux, cela entraînera-t-il une hausse des prix telle que les entreprises ne pourront plus s'assurer contre les cyberattaques ? L'assurance est-elle vraiment nécessaire lorsqu'une cyberprotection solide est installée en amont ? Plus simplement, la cyberassurance est-elle la meilleure solution à la cyberattaque ?

Un retard à combler par rapport aux Etats-Unis

« Au sein de notre groupe international, le premier produit de cyber-assurance a vu le jour dès 1998 aux Etats-Unis. Il faut cependant attendre septembre 2012 pour que son équivalent naisse en France », rappelle Sophie Parisot, product leader cyber d'AIG en France. En cause, le manque d'attaques en France par rapport au voisin américain. « Les objets connectés qui intéressent les cybercriminels sont arrivés tard en Europe », explique Michael Bittan, associé responsable des activités de gestion des risques cyber chez Deloitte. Le risque étant moins présent sur le vieux continent, les polices d'assurance avaient moins de raisons de se développer.

Et puis, il y a aussi les réglementations européennes. Aux Etats-Unis, le cadre juridique est plus adapté qu'en Europe en ce qui concerne le marché des cyberassurances. La donne est cependant en train de changer. Le 25 mai 2018 entrera en vigueur le règlement européen sur la protection des données (RGPD) qui obligera les professionnels à augmenter leur niveau de cybersécurité.

« En France, la cyberdélinquance est de plus en plus présente. Les technologies d'attaques sont disponibles en ligne ou sur le dark web. L'article 32 du RGPD oblige à mettre en place des systèmes de sécurité pour protéger les données personnelles. Quant à l'article 33, il contraint dorénavant à notifier à la CNIL les failles de sécurité », précise Alain Bensoussan, avocat à la Cour d'appel de Paris spécialisé en droit de l'informatique et des technologies avancées. S'ils ne suivent pas les nouvelles directives, les grands groupes pourront être condamnés à une amende représentant jusqu'à 4% de leur chiffre d'affaires ou 20 millions d'euros...[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : *Cyberattaques: pourquoi s'assurer n'est pas la meilleure solution – Challenges.fr*

Les clefs pour identifier un escroc sur Internet



Si souvent les femmes sont prises pour cible, l'adolescent, le retraité ou encore la working girl divorcée peuvent aussi se faire piéger. Lorsque la vérité éclate, il est difficile de s'en sortir : l'ado ne sait pas comment avouer qu'il est victime de chantage à la webcam sexuelle ou le retraité que sa belle arlésienne est partie avec ses économies. Tous doivent faire face à la honte et l'humiliation. Cet ouvrage décrypte les mécanismes de l'escroquerie sentimentale. Extrait de « Amour, emprise et manipulation sur internet » de Stéphanie Vigne, publié aux éditions Eyrolles.

Comme vous l'avez vu précédemment, l'association AVEN possède une base de données récoltant toutes les photos usurpées qu'elle a recensées depuis de nombreuses années. Ces photos sont utilisées par les fraudeurs pour créer de faux profils. En vous rendant sur <http://escrocs-love.e-monsite.com> et www.faux-profils.fr, vous pourrez vérifier la photo de votre interlocuteur. Si elle est sur la base de données, cela veut dire que c'est un faux profil.

Un autre moyen pour vérifier les photos est d'utiliser comme moi Google Recherche par images (voir plus haut page 125). Vous téléchargez la photo de votre correspondant dans l'espace de Google Recherche par images et vous accéderez ainsi à tous les sites où se trouve cette image. Si votre interlocuteur est un escroc, vous constaterez que la photo est sur différents sites et qu'elle est associée à différents noms.

Concernant mon escroc, j'ai vu qu'une des photos se trouvait sur un site canadien en rapport avec une conférence. J'ai trouvé un nom de personne lié à cette conférence et j'ai fait des recherches plus avancées. Je suis alors tombée sur un profil Facebook avec toutes les photos que mon fraudeur m'avait envoyées. Il paraissait évident que le détenteur de ce profil était bien la vraie personne et que le soi-disant Gregory avait volé ses photos.

Sur les sites de rencontre, les faux profils sont souvent « trop parfaits »...[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRIEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Manipulation, risque de détournement de vos données personnelles : les clefs pour identifier un escroc sur Internet* | Atlantico.fr

Assange a tenté de prévenir Clinton d'une cyberattaque imminente



Assange a
tenté de
prévenir
Clinton
d'une
cyberattaque
imminente

Dans un nouveau documentaire sur Julian Assange, sorti ce samedi, la réalisatrice évoque un épisode où le fondateur de WikiLeaks essayait, en vain, d'avertir Hillary Clinton de cyberattaques contre le Département d'État.

Le fondateur de Wikileaks Julian Assange aurait téléphoné au Département d'État américain pour avertir la secrétaire d'État Hillary Clinton d'une cyberattaque imminente contre les réseaux électroniques de la structure. La bande-annonce du documentaire «Risk», réalisé par Laura Poitras, en parle.

Le film, a été diffusé par la chaîne Showtime samedi 22/07/2017, et débute par un coup de fil d'Assange au Département d'État. Le lanceur d'alerte tente de parler personnellement à Hillary Clinton pour l'avertir que des mots de passe et divers fichiers ont été diffusés à travers le monde, raconte la voix off de la réalisatrice.

[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Assange a tenté de prévenir Clinton d'une cyberattaque imminente – Sputnik France*

Piratage de Office365 de Microsoft



Piratage
de
Office365
de
Microsoft

Selon le spécialiste de la gestion des accès dans le Cloud Skyhigh Networks, un assaillant non identifié s'est lancé, depuis le début 2017, dans une campagne d'accès frauduleux au service Office365 de Microsoft. L'opération cible des entreprises et vise à tenter de prendre possession des accès d'employés de haut niveau, pour récupérer des informations sensibles.

Skyhigh affirme avoir identifié plus de 100 000 tentatives (échecs d'authentification), émanant de 67 IP et dirigées contre 48 organisations utilisant le service SaaS. La société explique, dans un billet de blog, qu'il s'agit là d'une attaque assez sophistiquée, les assaillants ciblant seulement certains profils, conservant un rythme de tentatives suffisamment discret pour ne pas générer d'alerte sur le service de Microsoft et lançant leurs attaques depuis d'autres services Cloud publics. Classiquement, les assaillants misent sur la réutilisation des mots de passe sur divers services pour forcer le verrou de l'authentification (à partir de listes de login / mots de passe récupérées ou achetées sur le Darknet) et essayent différentes constructions pour 'deviner' l'adresse mail de chaque cible. Skyhigh indique toutefois n'avoir à ce jour aucune preuve d'une compromission de compte ou d'un éventuel vol de données...[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRETF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : Télégrammes : Amazon renforce Alexa ; Ethereum braqué

; Force brute contre Office365, Fusion Broadcom-Brocade compromise

Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed



Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed

Check Point Software Technologies Ltd révèle que 28 % des entreprises dans le monde ont été affectées par la campagne de publicités malveillantes RoughTed en juin, selon son tout dernier indice des menaces.

Check Point Software Technologies Ltd révèle que 28% des entreprises dans le monde ont été affectées de près ou de loin par la campagne de publicités malveillantes RoughTed en juin, selon son tout dernier indice des menaces.

RoughTed est une campagne de publicités malveillantes à grande échelle utilisée pour diffuser des sites web malveillants et des charges embarquées malveillantes telles que des escroqueries, des logiciels publicitaires, des kits d'exploitation de vulnérabilités et des logiciels rançonneurs. Elle a connu une forte poussée fin mai, puis a continué de se répandre en juin, touchant des entreprises dans 150 pays.

Large éventail

Les entreprises les plus touchées par RoughTed font partie des secteurs de la communication, de l'éducation, de la vente au détail et du commerce de gros... Les taux d'infection liés aux publicités malveillantes ont augmenté au cours des derniers mois, car il suffit aux pirates d'infecter une seule plate-forme de publicités en ligne pour atteindre un large éventail de victimes sans trop d'efforts, et il n'est pas nécessaire de se doter d'une infrastructure de diffusion lourde pour le logiciel...

En seconde place, Fireball, qui a touché 20% des entreprises en mai, a fortement reculé et n'a affecté que 5% des entreprises en juin. Le ver Slammer est la troisième variante la plus courante, touchant 4 % des entreprises...[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : *Cyberattaque : 28% des entreprises dans le monde ont été touchées par RoughTed*

Il diffusait des dizaines de données personnelles piratées sur Internet



Il diffusait
des dizaines
de données
personnelles
piratées sur
Internet

L'information provient de la plateforme Pharos qui permet à tout le monde de signaler un contenu suspect ou illicite sur Internet.

En février 2014, les forces de police s'intéressent donc à un site qui diffuse des dizaines de données personnelles piratées dont des numéros de carte bancaire et des scans de carte d'identité. La brigade de lutte contre la cybercriminalité de Lens est saisie. Les policiers remontent jusqu'à un habitant de Nœux-les-Mines. Convoqué au commissariat, il reconnaît avoir un certain attrait pour la sécurité des réseaux Internet.

Suite à une perquisition, son ordinateur est saisi. Et là, les découvertes s'enchaînent. En plus des données personnelles piratées, les enquêteurs retrouvent également plusieurs logiciels de piratage qui permettent de prendre le contrôle sur des sites mais aussi sur des ordinateurs à distance et, enfin, de modifier le contenu de bases de données.

Une cinquantaine de victimes

Autant de faits qui constituent des délits. Le mis en cause, 25 ans, est aujourd'hui poursuivi pour six d'entre eux.

Si le dossier a mis autant de temps à être bouclé c'est aussi qu'il fallait retrouver l'ensemble des victimes. Et elles sont nombreuses. Une cinquantaine a été retrouvée à ce jour, dont l'entreprise d'informatique Microsoft.

Autant de personnes face auxquelles le prévenu devra s'expliquer lors de l'audience correctionnelle prévue le 5 septembre.

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : *Il diffusait des dizaines de données personnelles piratées sur Internet – La Voix du Nord*

Découvrez tout ce que Google sait de vous



Le géant de la recherche vient d'inaugurer une nouvelle page, limpide et fonctionnelle, pour vous faciliter la vie.

La page Google Mon activité

La nouvelle page *Google Mon activité* est désormais le point de rendez-vous par excellence à l'heure de décortiquer tout ce que Google archive à votre sujet.

+ [Cliquez ici pour accéder à la page Google Mon activité](#)

Les yeux ébahis, vous découvrez minute par minute, heure par heure, jour par jour, **l'enregistrement détaillé de vos activités** au cœur des services Google. Sont encodées vos activités et vos recherches sur: Android, Chrome, Google Maps, Recherche, Recherche d'images, Recherche de vidéos, Trajets Google Maps, YouTube.



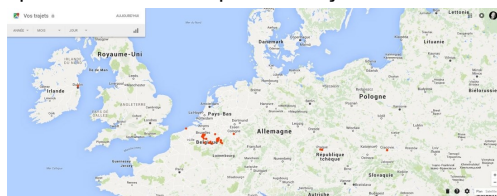
Le 5 juillet, Google à l'affût a gardé la trace tangible de 358 activités sur notre compte Google, via le navigateur Chrome, la recherche, YouTube...PHOTO: CAPTURE D'ÉCRAN

Consulter l'historique de vos trajets

En marge de cet archivage obsessionnel, Google se fait fort d'**enregistrer vos déplacements** via la puce GPS de votre smartphone et/ou de votre tablette.

«Redécouvrez les lieux que vous avez visités et les itinéraires que vous avez empruntés dans l'historique de vos trajets», positive le moteur de recherche.

+ [Cliquez ici pour consulter l'historique de vos trajets associé à votre compte Google](#)



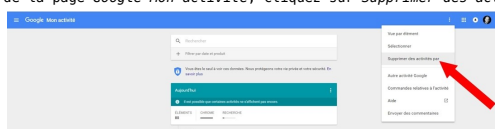
Les points rouges sur la carte montrent tous les endroits où Google vous a identifié grâce à la puce GPS de votre appareil mobile. PHOTO: CAPTURE D'ÉCRAN
La plate-forme pousse le vice jusqu'à présenter le classement des «lieux que vous fréquentez le plus souvent».

Effacer des données archivées

Vous souhaitez éclaircir, voire supprimer, cet archivage effréné de vos données personnelles?

Soulagement, la page *Google Mon activité* vous en laisse la possibilité, sans vous mettre des bâtons dans les roues.

À partir de la page *Google Mon activité*, cliquez sur *Supprimer des activités par*



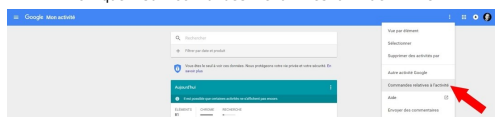
La section Supprimer des activités par vous permettra d'effacer partiellement ou totalement les données personnelles archivées par Google. PHOTO: CAPTURE D'ÉCRAN

Limiter la collecte des données

Une fois le nettoyage de printemps bouclé, libre à vous de **limiter partiellement ou autant que possible la collecte des données personnelles**.

Prenez à nouveau la direction de la page *Google Mon activité*.

Cliquez sur *Commandes relatives à l'activité*



Via la section Commandes relatives à l'activité, vous pourrez brider l'espionnage de Google. PHOTO: CAPTURE D'ÉCRAN

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;
RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DCTEP n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert
INFORMATIQUE
Cybersécurité & Conformité

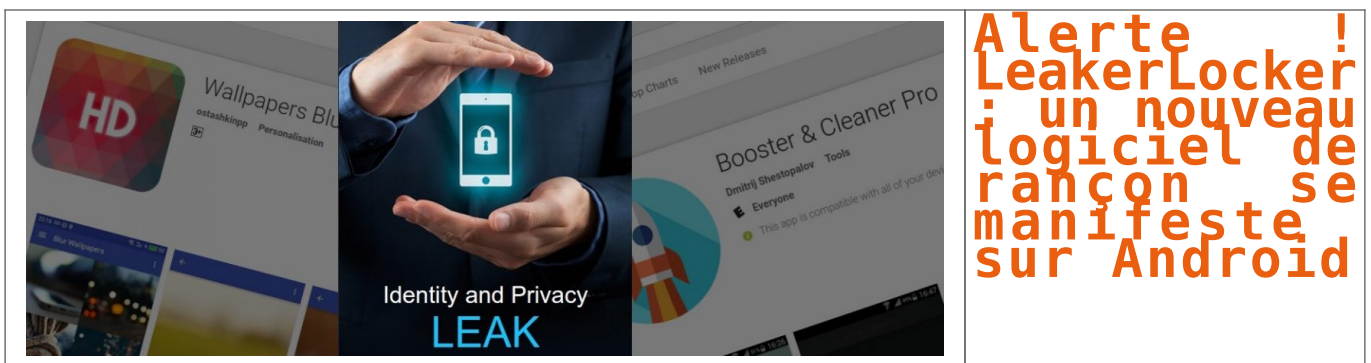
Contactez-nous



Réagissez à cet article

Source : *Voici comment consulter tout ce que Google sait de*

Alerte ! LeakerLocker : un nouveau logiciel de rançon se manifeste sur Android



Android doit faire face à un nouveau ransomware qui menace de dévoiler des informations compromettantes sur l'utilisateur du smartphone.

Android est le système d'exploitation le plus utilisé. Il est donc la cible de nombreux logiciels malveillants, c'est le cas de LeakerLocker. **Ce dernier est un ransomware, autrement dit un logiciel de rançon qui récupère des informations personnelles, menaçant de dévoiler leurs contenus si une certaine somme d'argent ne lui est pas versée.** LeakerLocker, quant à lui est un logiciel de rançon qui promet de vous humilier. **Pour cela, il utilise les données de votre historique de recherches et menace de l'envoyer à vos contacts.** Le montant de la rançon s'élève à 50 euros. Un logiciel de rançon d'un nouveau genre fait son apparition sur Android.

Un logiciel de rançon apparu en premier lieu sur Android

McAfee, le logiciel antivirus stipule que ce logiciel malveillant est né sur le système d'exploitation Android. **Il se propage avec l'installation de deux applications disponible sur Google Play : Booster & CCleaner Pro ainsi que Wallpapers Blur HD.** Il réussit à dérober des informations qui pourraient vous nuire, au sein de votre smartphone afin de les utiliser contre vous...[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : *LeakerLocker : un nouveau logiciel de rançon se manifeste sur Android*

Les points faibles du Ransomware Petya/NotPetya



Les points
faibles du
Ransomware
Petya/NotPetya

Alors que le mystère s'épaissit sur les intentions réelles des auteurs du malware parti d'Ukraine fin juin, des chercheurs d'une société de sécurité informatique britannique sont parvenus à décrypter des fichiers endommagés sur une machine infectée.

Jusqu'à présent, toutes les actions entreprises pour récupérer les données attaquées par NotPetya sont vouées à l'échec.

Erreur de programmation de l'algorithme de cryptage

Un maigre espoir pour les victimes du malware Petya/NotPetya : sur leur blog les chercheurs en cybersécurité de la société britannique Positive Technologies expliquent avoir réussi à décrypter des fichiers endommagés sur un ordinateur infecté. Très ardue, la procédure de récupération ne serait possible que sur certaines machines, celles dont le virus a encrypté les droits d'administrateur. Une découverte fort intéressante, alors que jusqu'à présent, personne, y compris les victimes ayant payé la rançon exigée par les attaquants, n'a pu récupérer ses données...

Positive Technologies a découvert plusieurs erreurs commises par les pirates dans la conception du malware, en particulier dans la programmation de l'algorithme de cryptage Salsa20. Au lieu d'utiliser une clé de chiffrement de 256 bits, ils se sont apparemment contentés d'une clé moins puissante de 128 bits, que Positive Technologies est parvenu à contourner pour récupérer certains fichiers....[lire la suite]

Notre métier : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec le RGPD (règlement Européen relatif à la protection des données à caractère personnel).

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)



Réagissez à cet article

Source : *Petya/NotPetya : des chercheurs ont découvert des points faibles*